

Norton AntiVirus™ for Lotus Notes™/Domino for Linux Implementation Guide



Norton AntiVirus™ for Lotus Notes™/Domino for Linux Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 2.5

Copyright Notice

Copyright © 1997–2002 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, Norton AntiVirus, Symantec AntiVirus for Macintosh, and Norton Utilities are trademarks of Symantec Corporation.

Windows is a registered trademark of Microsoft Corporation. Lotus and Lotus Notes are registered trademarks of Lotus Corporation. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC CORPORATION SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE.

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

- A. use that number of copies of the Software as have been licensed to you by Symantec under a License Module, provided that if the Software is part of a suite of Symantec software licensed to you, the number of copies you may use of all titles of the software in the suite, including the Software, may not exceed the total number of copies so indicated in the License Module in the aggregate, as calculated by any combination of licensed suite products. Your License Module shall constitute proof of your right to make such copies. If no License Module accompanies, precedes, or follows this license, you may make one copy of the Software you are authorized to use on a single computer.
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;
- C. use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network; and
- D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

YOU MAY NOT:

- A. copy the printed documentation which accompanies the Software;
- B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon

upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

F. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any product for which you have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

4. DISCLAIMER OF DAMAGES:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software"

and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

6. GENERAL:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Service, 555 International Way, Springfield, OR 97477.

Contents

Norton AntiVirus for Lotus Notes/Domino

About Norton AntiVirus	8
What is a computer virus?	8
How Norton AntiVirus works	9
Installing Norton AntiVirus for Lotus Notes	10
Minimum system requirements for Linux	10
Installation	11
Securing the Norton AntiVirus databases	13
Uninstalling	14
Replicating the NAV Settings and NAV Log databases	15
Replicating the NAV Definitions database	17
Starting Norton AntiVirus for Lotus Notes	19
Using the Notes console window	20
Configuring scanning	21
Scheduling scans	23
Setting Global Options	24
Using the NAV Log	28
Managing the Quarantine	31
Maintaining current protection	35
About LiveUpdate	35
How to update virus protection	35
Configuring for an internal LiveUpdate server	37

Service and support solutions

Index

Norton AntiVirus for Lotus Notes/Domino

This guide contains the following topics:

- [About Norton AntiVirus](#)
- [Installing Norton AntiVirus for Lotus Notes](#)
- [Starting Norton AntiVirus for Lotus Notes](#)
- [Configuring scanning](#)
- [Using the NAV Log](#)
- [Maintaining current protection](#)

About Norton AntiVirus

Norton AntiVirus secures your Lotus Notes environment against virus attacks by protecting databases on Lotus Domino servers and monitoring email that is routed through the servers. Norton AntiVirus operation is transparent to users, with minimal performance degradation to the network.

However, the Lotus Notes environment is only one avenue a virus can use to penetrate your site. For a complete virus protection solution, make sure the appropriate workstation or server version of Norton AntiVirus is installed on every computer at your site as well.

Norton AntiVirus (NAV) is completely integrated into the Lotus Notes environment. All scanning is configured and initiated from the NAV Settings database. All reports and virus dispositions are handled through the NAV Log database. Information about the product and how to use it is provided in the NAV Help database.

Norton AntiVirus for Lotus Notes can be configured to do any of the following:

- Eliminate viruses automatically on detection.
- Quarantine infected documents and email for administrator review.
- Delete infected items.

When viruses are detected, email notifications are sent, optionally, to specified administrators, document or email authors, and intended email recipients.

What is a computer virus?

A computer virus is a program designed in such a way that, when run, it attaches a copy of itself to another computer program or document. Thereafter, whenever the infected program is run or the infected document is opened, the attached virus program is activated and attaches itself to yet other programs and documents.

In addition to replicating, viruses are generally programmed to deliver a payload. Most viruses simply display a message on a particular trigger date. Some, however, are programmed specifically to damage data by corrupting programs, deleting files, or reformatting disks.

Two classes of viruses compose the greatest threat in the Lotus Notes environment:

- Macro viruses, which infect word processing and spreadsheet documents (such as Microsoft Word or Excel)
- Program viruses, which infect executable files

The viruses spread as attachments to documents written to Notes databases on servers and Notes email. Norton AntiVirus for Lotus Notes detects and eliminates these viruses.

How Norton AntiVirus works

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. Once a virus is identified, information about the virus (a virus signature) is stored in a virus definitions file, which contains the necessary information to detect and eliminate the virus. When Norton AntiVirus scans for viruses, it is searching for these telltale virus signatures.

To supplement detection of known viruses, Norton AntiVirus includes a powerful new component called Bloodhound. With this advanced heuristic technology, Norton AntiVirus can detect a high percentage of new or unknown viruses not yet analyzed by anti-virus researchers.

The Norton AntiVirus LiveUpdate feature makes sure your virus protection remains current. Updated virus definitions files are provided by Symantec regularly. With LiveUpdate, Norton AntiVirus connects automatically to a special Symantec site, determines if your files need updating, downloads the proper files, and installs them in the proper location.

Installing Norton AntiVirus for Lotus Notes

The Norton AntiVirus setup program creates a directory named symantec that contains Norton AntiVirus products (shared libraries and executable files). By default, the symantec directory is installed to /opt, however, during install you can specify a different location. In addition, Norton AntiVirus also creates the following directories:

- .../Symantec/NavNotes/bin
Norton AntiVirus engine
- <Domino server’s default data directory>/nav
Norton AntiVirus databases (nav.nsf, navlog.nsf, and navhelp.nsf)
- .../Symantec/virusdefs
Virus definitions files that are specific for the operating system
- .../Symantec/LiveUpdate
Technology to download virus definitions files and program updates

Minimum system requirements for Linux

Administrator-level privileges to both Linux and the Lotus Domino server are required to install Norton AntiVirus for Lotus Notes/Domino for Linux.

Operating systems	Redhat versions 6.2 and 7.3 SuSE 7.3
	Note: Although testing has not been completed for other Linux versions, preliminary results indicate that Norton AntiVirus for Lotus Notes should operate properly. Other versions are neither certified nor supported.
Lotus Notes	Domino Server R5 versions 5.0.9 or higher
Available disk space	200 MB disk space on the partition on which Norton AntiVirus for Lotus Notes is installed

Installation

Older versions of Norton AntiVirus for Lotus Notes should be uninstalled before installing. See [“Uninstalling”](#) on page 14, if necessary.

For Norton AntiVirus for Lotus Notes to function properly, the avdefs group must exist. This can be accomplished in two ways:

- The avdefs group exists on the computer on which the Domino server runs.
- The avdefs group is valid on the computer on which the Domino server runs. For example, the avdefs group is maintained on an NIS server and the computer on which the Domino server runs on has access to those NIS controlled accounts.

The avdefs group can be created and populated at install time by the Norton AntiVirus for Lotus Notes installation script, or you can create the group and add Notes users manually before performing the Norton AntiVirus for Lotus Notes installation. The installation script will not complete if the avdefs group does not already exist or you do not allow the installation script to create the group itself.

Note: All Domino server user accounts (server user IDs) that are going to have Norton AntiVirus for Lotus Notes installed into their respective Notes partitions must be added as members of the avdefs group.

After installation, when Domino users have been added to the avdefs group, any terminal sessions launching Domino must be logged off and logged in fresh to ensure that the group membership and associated permissions are enabled. Failure to do this prevents Norton AntiVirus from locating virus definitions on startup, and, subsequently, not loading completely.

To install Norton AntiVirus for Lotus Notes/Domino for Linux

- 1 Shut down the Lotus Domino server.
- 2 Shut down the Lotus Notes client.
- 3 Go to CD-ROM directory (cd /cdrom).
- 4 Run the shellscript ./install from the Norton AntiVirus CD-ROM.

Note: If you have multiple Lotus Notes partitions on the same server, separate Norton AntiVirus databases are required for each partition. Setup detects and lets you specify on which partitions to install Norton AntiVirus.

- 5 After the Norton AntiVirus install completes, restart the Lotus Domino server.
When the Lotus Domino server is restarted, the Norton AntiVirus databases are created from templates and placed in the nav sub-directory of your default Data directory. A readme.txt file is placed in this directory as well.
- 6 Select the workspace tab on which you want to place Norton AntiVirus. Some administrators prefer to label and dedicate a single tab to Norton AntiVirus.
- 7 From the File menu, choose Database, then Open.
- 8 Select the appropriate server. In the nav folder, open the NAV Settings database.

Install script options

The install shellscript can install Norton AntiVirus for Lotus Notes either interactively or non-interactively:

- Interactively: No command-line options are supplied.
- Non-interactively: The -p and -s options are specified on the command line.

Syntax

```
./install [-h] [-p <notespartition>] [-s <Symantec base directory>] [-d]
```

Options

- | | |
|----|--|
| -h | Displays the command-line syntax. |
| -p | Specifies the full path to the Notes partition on which to install Norton AntiVirus. Multiple Notes partitions, separated with commas, can be specified. |
| -s | Specifies the full path to the Symantec base directory that will contain all the Norton AntiVirus for Lotus Notes binary files.

The -s option cannot be used on its own; it is used only in conjunction with the -p option. |
| -d | Specifies that the Norton AntiVirus for Lotus Notes installation process should use default settings.

The -d option must be specified if the avdefs group does not yet exist or the install will fail. |

The following example installs Norton AntiVirus for Lotus Notes to two Notes partitions in the default Symantec directory:

```
./install -p /notesdata1,/notesdata2 -d
```

Securing the Norton AntiVirus databases

To secure your Norton AntiVirus databases after installation, perform the following tasks for both the nav.nsf and navlog.nsf databases:

- Modify the Access Control List to restrict access to anti-virus or Lotus administrators only.
- Sign the databases with a Trusted ID from your organization to maintain the security of the Execution Control List of Notes clients that access the databases.

To set Access Control

- 1 Right-click the NAV Settings database icon and choose Database > Access Control from the pop-up menu.
- 2 Select users and grant them Manager access with Delete rights.
- 3 Repeat the procedure for the NAV Log database.

Be sure to keep Manager access for the server group LocalDomainServers or Norton AntiVirus will not operate properly.

To maintain security for the Execution Control List of Notes clients

- ◆ Properly sign the NAV Settings (nav.nsf) and NAV Log (navlog.nsf) databases with a Trusted ID.

For information on signing databases, search the Domino Administrator help database for the “tools - database - sign” topic.

Uninstalling

Uninstalling Norton AntiVirus version 2.1

Root-level privileges are required to uninstall Norton AntiVirus.

To remove Norton AntiVirus version 2.1

- 1 Stop the Domino server.
- 2 Switch to superuser or equivalent.
- 3 Change to the /opt/lotus/notes/symantec/uninstall/ directory.
- 4 Type the following at the command prompt:
./uninstallnav
- 5 Follow the prompts.
- 6 After the uninstall completes, exit superuser state and restart the Domino server.

Note: To verify that Norton AntiVirus is uninstalled, examine the server's notes.ini file. The line NSF_HOOKS=nhook should not be present and nntask should be removed from the ServerTasks line.

Uninstalling Norton AntiVirus version 2.5

Norton AntiVirus 2.5 now has the ability to share components with other Symantec products. If Norton AntiVirus detects that the shared components are in use those files will not be removed during the uninstall process. This ensures that other Symantec products that use these components will still function correctly after Norton AntiVirus for Lotus Notes is uninstalled.

Additionally, backup files are not removed during the uninstall process. Norton AntiVirus for Lotus Notes makes a backup file of any existing file that gets written to or changed during the installation process. For example, the notes.ini file located in the ../<notesdata> directory is modified during the installation process. As a courtesy to administrators, a backup of the original notes.ini file is created. The backup file is called notes.ini.symbak and is not removed during the uninstall process.

To remove Norton AntiVirus version 2.5

- 1 Stop the Domino server.
- 2 Switch to superuser or equivalent.
- 3 Change to the .../Symantec/NavNotes/uninstall directory.
- 4 Type the following at the command prompt:
./uninstallnav
- 5 Follow the prompts.

After the uninstall completes, you can manually remove backup files. Leaving these files, however, will not affect server performance. The following files may need to be removed manually.

- /etc/group.symbak
- /etc/liveupdate.conf.symbak
- /etc/Symantec.conf.symbak
- .../<notesdata>/notes.ini.symbak

Replicating the NAV Settings and NAV Log databases

The NAV Settings database, nav.nsf, can be replicated to other Domino servers running Norton AntiVirus for Lotus Notes 2.5. The NAV server task, nntask, monitors nav.nsf for changes to the NAV settings through replication and reloads the settings on the local server. NAV settings can be distributed by manual or scheduled replication.

The following subset of settings in the NAV Settings database are replicated between Domino servers:

- Auto-Protect settings
- Global options settings
- All scheduled scans

See [“Configuring scanning”](#) on page 21 for information about NAV settings.

The NAV Log database, navlog.nsf, stores server messages, reports of virus incidents, and scan summaries. It also provides access to quarantined documents and documents Norton AntiVirus backs up before eliminating viruses. Through replication, you can maintain a master NAV Log that automatically includes virus incidents and statistics reports from other Domino servers running Norton AntiVirus. See [“Using the NAV Log”](#) on page 28 for information about the NAV Log.

Before Norton AntiVirus is installed

To prepare for NAV Settings and NAV Log replication

- 1 Select a server in your organization to be the master Norton AntiVirus server.
- 2 Install Norton AntiVirus for Lotus Notes/Domino for Linux on the server and start the Domino server on that machine.
- 3 Ensure that Notes administrators and LocalDomainServers are in the Access Control List of nav.nsf and navlog.nsf, with Manager access and Delete Documents enabled. The LocalDomainServers group should contain all of the servers to which you plan to replicate.
- 4 Before installing Norton AntiVirus/Domino for Linux on other servers, create replicas of the newly installed nav.nsf and navlog.nsf databases in the nav directory in the default data directory of the other Domino servers.
- 5 Install Norton AntiVirus for Lotus Notes on the other servers, but keep the already replicated nav.nsf and navlog.nsf databases. This is an option of the Norton AntiVirus setup program.

Any changes made to NAV settings on any of the Domino servers are distributed to the other replicas when a manual or scheduled replication occurs. After replication, the new NAV settings are reloaded automatically.

Note: Replication conflicts can be avoided by permitting only the Notes administrator in charge of antivirus policy to edit the NAV settings on each of the Domino servers.

For the log, initiate push replication from the NAV Log replicas to the master navlog.nsf. In this way, logging of virus incidents across the network is centralized.

After Norton AntiVirus is installed

If Norton AntiVirus for Lotus Notes is already installed on a Domino server to which the NAV Settings or NAV Log databases are being replicated, you must stop the NAV server task on that server before replicating the database.

To stop the NAV server task on a replica Domino server

- 1 Type tell nav quit in the server console window.
- 2 Replicate the NAV Settings and NAV Log databases from the master Domino server to the replica Domino servers.
If prompted to overwrite an existing nav.nsf or navlog.nsf, respond Yes. This overwrites the existing databases with the new replicas.
- 3 Type load nntask to restart NAV.

Replicating the NAV Definitions database

The NAV Definitions database, navdefs.nsf, stores updated virus definitions. The database can be replicated to other Domino servers running Norton AntiVirus for Lotus Notes 2.5 so that only a single LiveUpdate is required to maintain current protection on all servers. See [“Maintaining current protection”](#) on page 35 for information.

The Domino server on which the master navdefs.nsf is created should be the machine that downloads new virus definitions updates through a scheduled LiveUpdate.

Caution: Never replicate navdefs.nsf to different operating systems. The processing engines are platform-specific.

Use of the NAV Definitions database is only required if you plan to replicate updated virus definitions to separate physical servers. Partitioned servers on the same physical server will update definitions within ten minutes of a new LiveUpdate download. If you do not intend to replicate virus definitions, you do not need to create the NAV Definitions database.

Caution: Never replicate navdefs.nsf to more than one partition of a multi-partition Domino server. Only one LiveUpdate per physical machine is required to update definitions on all partitions of that machine.

To prepare NAV Definitions for replication

- 1 Select a Domino server in your organization that will be used to download updated virus definitions.
- 2 After installing Norton AntiVirus on the server, click LiveUpdate in the Norton AntiVirus main window.
- 3 In the LiveUpdate form, click Create NAV Definitions Database.
- 4 Enable and schedule the LiveUpdate.
- 5 Make sure that Save Downloaded Virus Definitions In The NAV Definitions Database is checked.
- 6 Ensure that you and LocalDomainServers are in the Access Control List of navdefs.nsf, with Manager access and Delete Documents enabled. The LocalDomainServers group should contain all of the servers to which you plan to replicate.
- 7 Create replicas of the master navdefs.nsf database on the other Domino servers running Norton AntiVirus (only one per physical machine).
The definitions database must be in the <Domino server data directory>/nav directory on the other Domino servers and be called navdefs.nsf.

The next time a scheduled LiveUpdate runs, any updated virus definitions are downloaded and a new navdefs.nsf document is created. The new virus definitions set is marked as active. The updated definitions are distributed to the other replicas when a manual or scheduled replication occurs. The NAV server task checks for a new virus definition set at 10 minute intervals.

After LiveUpdate runs and updates the master navdefs.nsf database, replicate the new virus definitions to other servers. Remember, only one navdefs.nsf should exist on a single machine, regardless of the number of Notes partitions with Norton AntiVirus installed.

To replicate virus definitions to other servers, do one of the following:

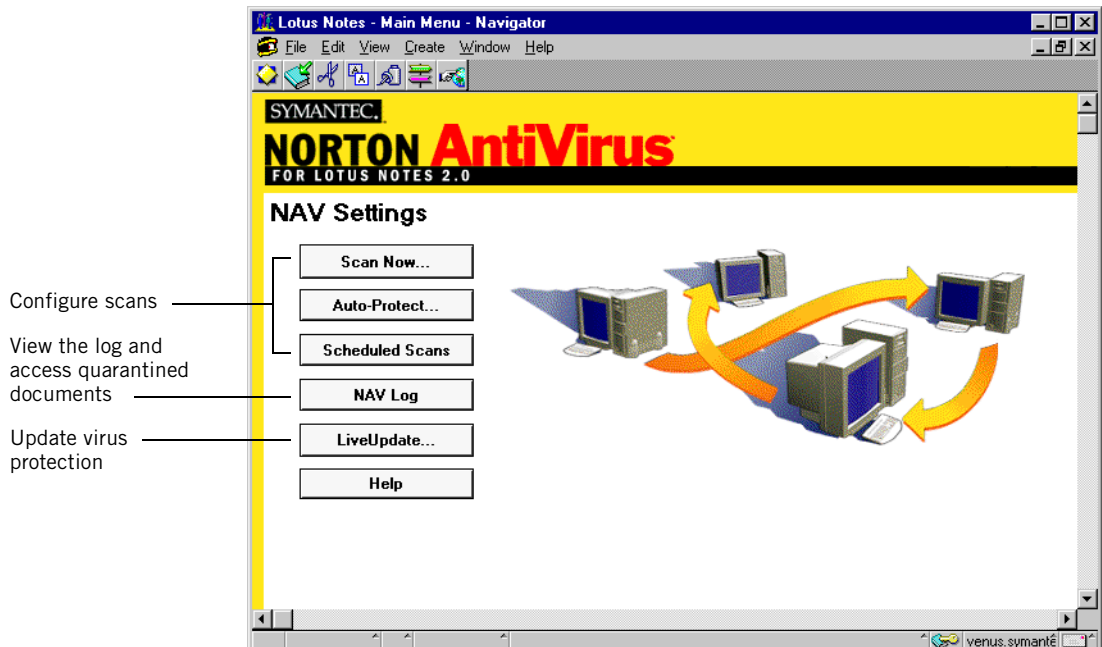
- Manually replicate the master navdefs.nsf to other Domino servers running Norton AntiVirus.
- Schedule the replication of the master navdefs.nsf to other Domino servers running Norton AntiVirus.

Starting Norton AntiVirus for Lotus Notes

Norton AntiVirus runs as a Domino server task. Every time the server is started, Norton AntiVirus protection begins as well. Management and configuration tasks are accessed through the Lotus Notes client.

To access Norton AntiVirus for Lotus Notes

- ◆ Double-click the NAV Settings icon on your Lotus Notes workspace tab.
 The first time you click the NAV Log and Help buttons, icons for these databases are placed on your Lotus Notes workspace tab as well.



To get help while using Norton AntiVirus, do any of the following:

- In the Norton AntiVirus main window, click the Help button to display the help table of contents.
- In the Action bar of any form or view, click the Help button to access the context-specific help topic.
- In any form, click the group label that precedes options for a brief pop-up description of the options.

Using the Notes console window

You can view and manage some Norton AntiVirus operations directly from the Domino server console window. Use the following syntax at the command prompt:

TELL NAV <command>

Command	Description
HELP	Lists Norton AntiVirus console commands.
INFO	Summary of Norton AntiVirus operation.
STAT RESET	Clears processing details.
JOBS	Lists upcoming scheduled scans. The job names are the ones entered when the scan was scheduled.
SCAN <names>	Initiates a scan of the specified databases. A number is displayed in the console window to identify each scan.
STOP <n>	Stops the scan with the specified number.
QUIT	Stops the Norton AntiVirus server process. To reload Norton AntiVirus, enter LOAD NTASK at the console command prompt.

Configuring scanning

Norton AntiVirus scans can be initiated at any time, scheduled to run at specific times, or set to monitor database writes and email routing in real time.

To configure and initiate scans

- 1 Double-click the NAV Settings icon on your Lotus Notes workspace tab to open the Norton AntiVirus main window.
- 2 In the Norton AntiVirus main window, click one of the following buttons to configure scanning:
 - **Scan Now**
 An on-demand scan you can invoke at any time. You can select either all databases in your default Data directory or select specific databases or directories to scan. The scan does not begin until you click Start The Scan in the form. You can also restrict the scan to documents that have been modified since a specified date.
 - **Auto-Protect**
 Real-time scanning of database writes on the server and email as it is routed through the server. Auto-Protect is your best insurance to detect and eliminate viruses before they have a chance to spread.
 - **Scheduled Scan**
 Scans that run automatically and without administrator intervention. Use scheduled scans to ensure that your databases remain virus-free. You can also restrict the scan only to documents that have been modified since the last scheduled scan.

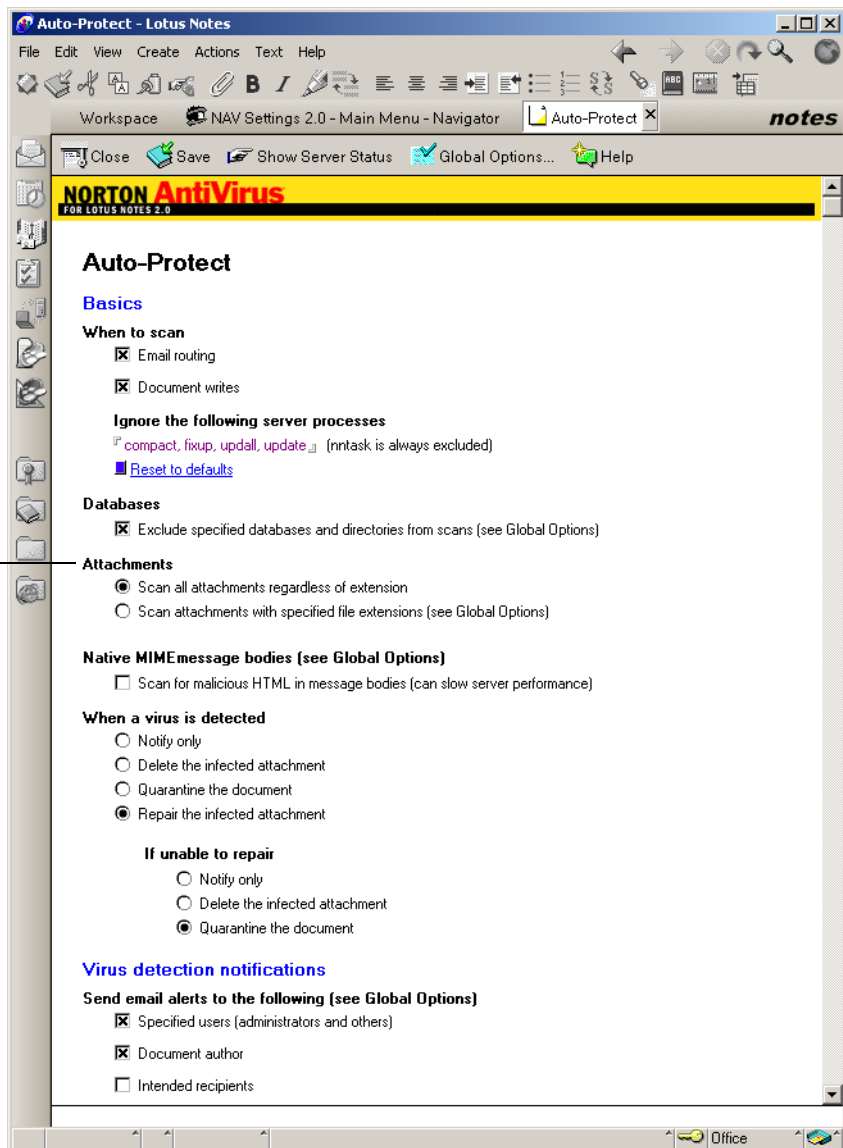
Each scan type uses a three-section form to configure the scan:

Basics	What and when to scan.
Scan Options	Which global options to apply and what to do if a virus is detected. Click the Global Options button in the Action bar of any form to modify settings.
Notifications	Whom to notify when a virus is detected. Click the Global Options button in the Action bar of any form to identify administrators and customize the body of the email notification.

As an example, the following figure shows the form to configure Auto-Protect real-time scanning. Click the option group labels for pop-up help about the options or click Help in the Action bar for detailed context help.

Auto-Protect scan form

Click the
group labels
for pop-up
help with
options

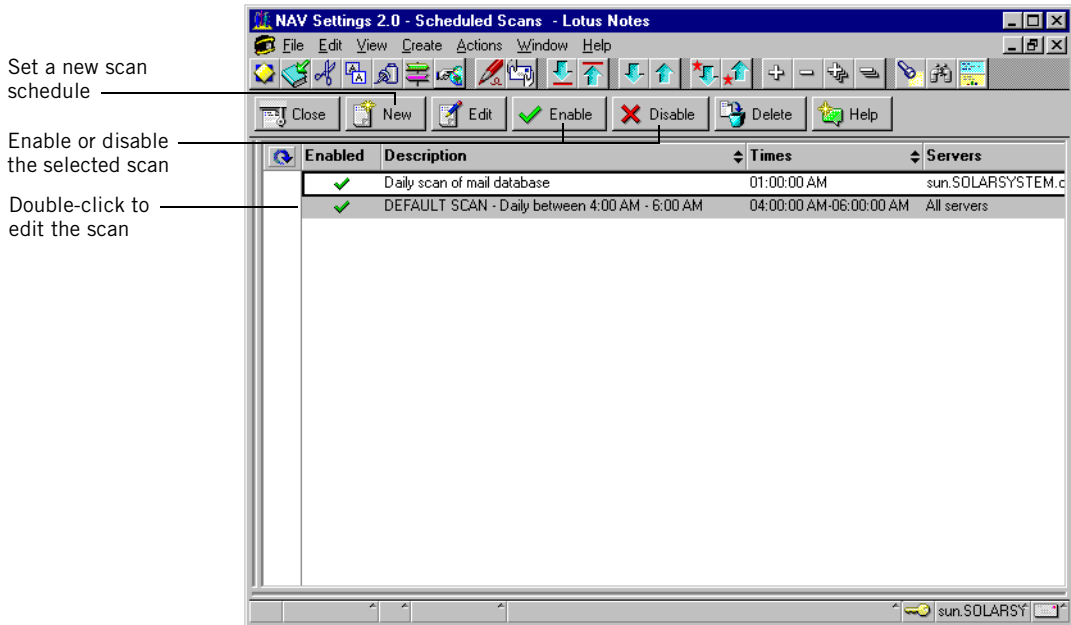


Scheduling scans

Scans can be scheduled to repeat at the same time on specified days.

To schedule scans

- 1 In the Norton AntiVirus Main window, click Scheduled Scans.
- 2 Do one of the following:
 - Double-click an existing scan to modify it.
By default, a scan of all databases in the Data directory of the server is configured to run daily at 4:00 A.M.
 - Click New to configure and schedule a scan.



When scheduling scans with Norton AntiVirus 2.5, you can specify a time range in which the scan runs as well as the start time for the scan. If all databases are not scanned during the specified time range when the scan runs, the scan continues after the last document scanned the next time the scan runs. This capability ensures coverage for sites with many large databases that don't have time to scan all selected databases during a single Scheduled Scan.

The time range is entered when scheduling the scan. For example, if 04:00 AM - 06:00 AM is entered, the scan starts at 04:00 AM. If the scan is not completed by 06:00 AM, the scan is stopped and continues where it left off at the next scheduled time. If a single start time is specified (for example, 09:00 AM), the scan continues to completion.

Note: For domains with multiple servers, there is a configuration option that lets you schedule the same scan to run on one or more servers. The scan itself can be scheduled from any server in the domain. For server-specific changes to scheduled scans, the nav.nsf database must be replicated to the appropriate servers.

Setting Global Options

Global options can be accessed and configured from any of the scan forms. These options apply to all scans. Changes made, for example, from the Scan Now form, apply to Auto-Protect and all previously scheduled scans. Once set, however, you probably do not need to change them.

To set global options

- 1 In the Norton AntiVirus main window, click Scan Now, Auto-Protect, or Scheduled Scan.
- 2 At the top of the scan form, click Global Options.
- 3 Set the options, which are summarized in the following tables.

4 Click Save, then Close.

Click the
group labels
for pop-up
help with
options

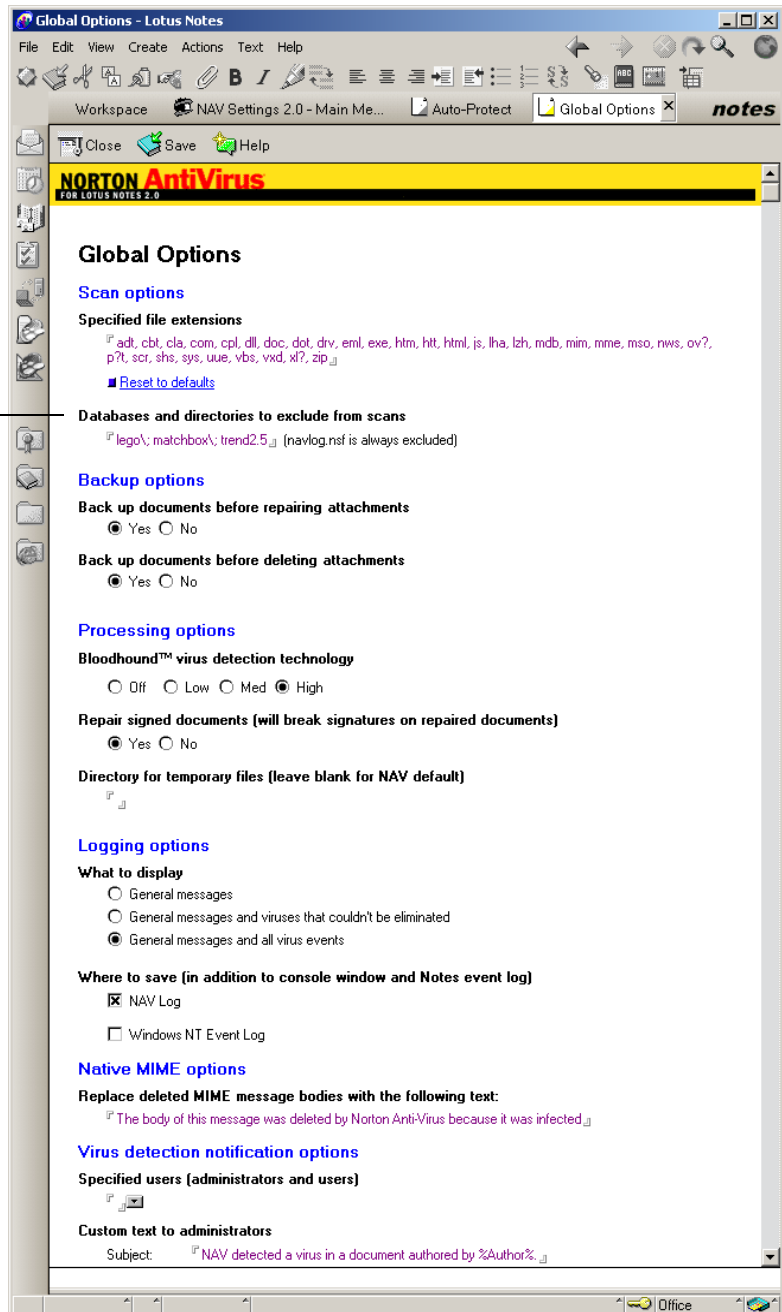


Table 1-1 Scan options

Specified file extensions	When configuring a scan (Scan Now, Auto-Protect, or Scheduled Scan) and Scan Attachments With Specified Extensions is selected, Norton AntiVirus only scans attachments whose file extensions are listed. This setting reduces resource demand and speeds processing during the scan. The default list includes file types commonly at risk of infection. If your environment includes executable files with non-standard extensions, add them to the list. In most cases, the default list is appropriate.
Databases and directories to exclude from scans	When configuring a scan (Scan Now, Auto-Protect, or Scheduled Scan) and Exclude Specified Databases And Directories From Scans is checked, Norton AntiVirus always skips the listed databases and directories. For example, you may have documentation or reference databases that are not at risk of virus infection because they cannot be modified by users.

Table 1-2 Backup options

Back up documents before repairing	As a data safety precaution, Norton AntiVirus can store a backup copy of an infected document before making the repair to eliminate the virus. In the NAV Log, click Backup Documents to view the list and delete or restore backups.
Back up documents before deleting	As a data safety precaution, Norton AntiVirus can store a backup copy of an infected document before deleting an infected attachment. In the NAV Log, click Backup Documents to view the list and delete or restore backups.

Table 1-3 Processing options

Bloodhound virus detection technology	Bloodhound is an advanced heuristic technology that detects a high percentage of any new or unknown viruses that have not yet been analyzed by anti-virus researchers. Because there is a small processing overhead, you can set the level of resource demand. In most cases, the Med (medium) setting is appropriate.
Repair signed documents	To eliminate viruses from signed documents, Norton AntiVirus must break the signature. If Repair Signed Documents is disabled and a virus is detected, a signed document is treated as one that cannot be repaired.
Directory for temporary files	For processing during scans, Norton AntiVirus uses the .../Symantec/temp directory. You can specify another directory. If you use another anti-virus product, disable scanning of this directory to prevent interference with Norton AntiVirus operation.

Table 1-4 Logging options

What to display	Determines what information is reported during Norton AntiVirus processing.
Where to save	Norton AntiVirus system information is always reported in the Domino server console window and stored in the Miscellaneous Events view of the Notes log. In addition, you can save this information in the Server Messages view of the NAV Log. The Windows NT Event Log option is provided for compatibility with the Windows NT version, should you choose to replicate to a Windows NT-based Domino server.

Table 1-5 Native MIME options

Replace deleted MIME message bodies	An additional feature in Norton AntiVirus 2.5 is the ability to scan Native MIME message bodies. This new feature allows an anti-virus administrator ability to enable scanning for malicious HTML code in message bodies (for example, the KAK-worm threat). The replacement text can be customized for your environment.
--	---

Table 1-6 Virus detection notifications

Administrators (and specified users)	Select administrators and other users who should be notified when a virus is detected. Use the email alert to advise them to attend to users whose workstations are infected.
Document authors	Use the email alert to instruct users how to eliminate the virus source, such as scanning with a workstation version of Norton AntiVirus.
Document recipients	If your policy is to quarantine infected documents, let users know whom to contact to release the document. If your policy is to delete infected attachments, advise them to contact the document author to resend an uninfected version.

Using the NAV Log

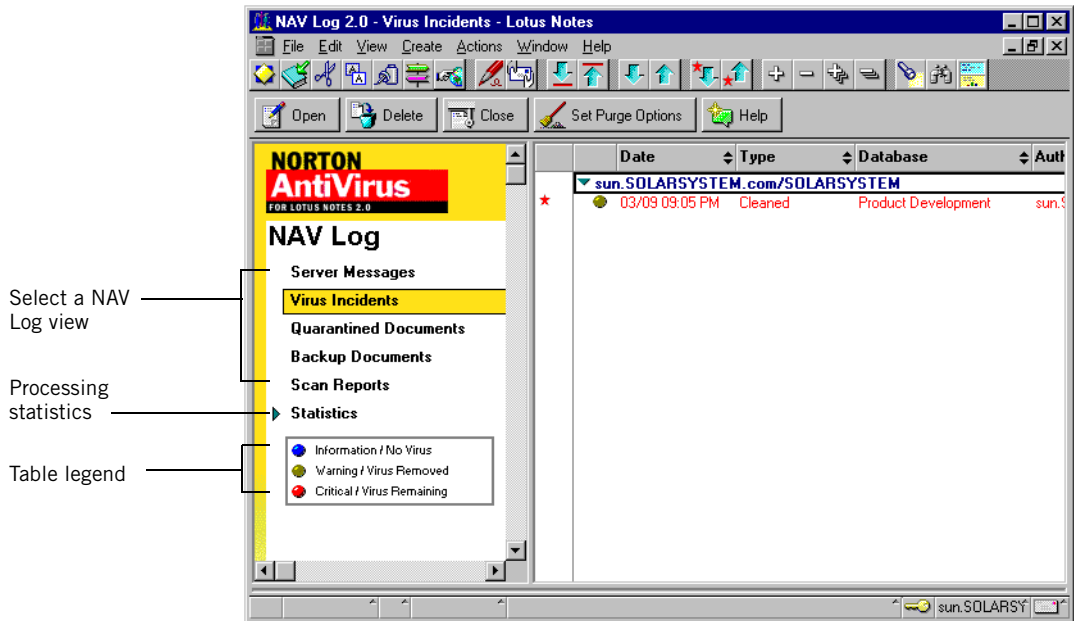
The NAV Log stores server messages, reports of virus incidents, and scan summaries. It also provides access to quarantined documents and documents Norton AntiVirus backs up before eliminating viruses.

To prevent the log from growing too large, a purge agent runs every night at 1:00 A.M. By default, Virus Incidents are purged after 365 days. Other NAV Log entries are purged after 30 days. To change the number of days that log entries are stored, open the NAV Log and click Set Purge Options on the Action Bar.

Note: Your current user account must have administrator-level privileges for agents on the server where NAV Log resides to enable the purge agent.

To access the NAV Log

- 1 Do one of the following:
 - Click the NAV Log icon on your Notes workspace tab.
 - In the Norton AntiVirus main window, click NAV Log.

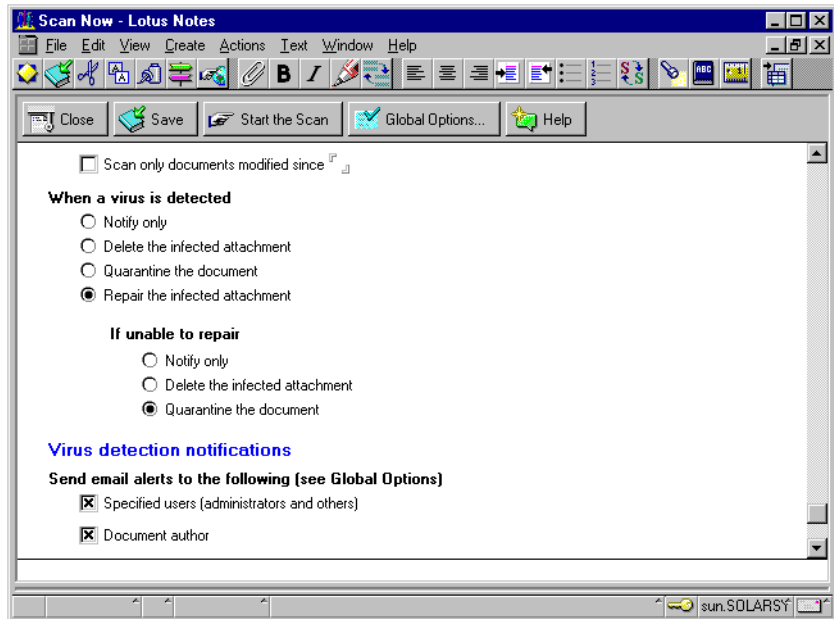


- 2 Click to select one of the following log views:
 - Server Messages
All server-related events.
 - Virus Incidents
All virus detections.
 - Quarantined Documents
Infected documents that have not been repaired.
 - Backup Documents
As a data safety precaution, Norton AntiVirus is configured by default (from Global Options) to store a backup copy of documents that contain infected attachments before attempting a repair or deleting documents.
 - Scan Reports
Summaries of scheduled and on-demand scans.
 - Statistics
Statistics for Norton AntiVirus processing.

Managing the Quarantine

When using the Scan Now, Auto-Protect, or Scheduled Scan forms to configure scans, indicate in the Scan Options section what to do if a virus is detected. The following figure shows this section of the form.

Figure 1-1 Scan Now, Auto-Protect, and Scheduled Scan forms

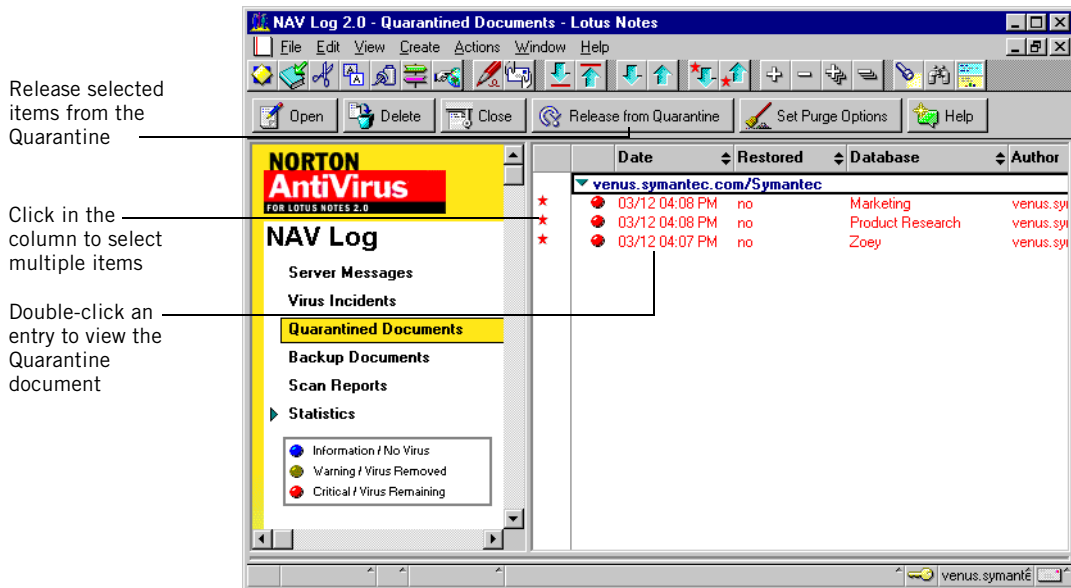


Documents are quarantined for one of two reasons:

- Your scan configuration is set to quarantine documents if a virus is detected.
- Your scan configuration is set to repair infected attachments, but quarantine any documents that have attachments that cannot be repaired.

To manage items in the Quarantine

1 Open the NAV Log and click Quarantine Documents.



2 Select an item in the list.

3 Do one of the following:

- Click Release from Quarantine.

Depending on the item, the database write is completed or the email is delivered. See the next procedure for information on how to handle infected attachments.

Make sure the document or email no longer contains infected attachments. If you release a document that still has infected attachments, it will be quarantined again.

- Click Delete.

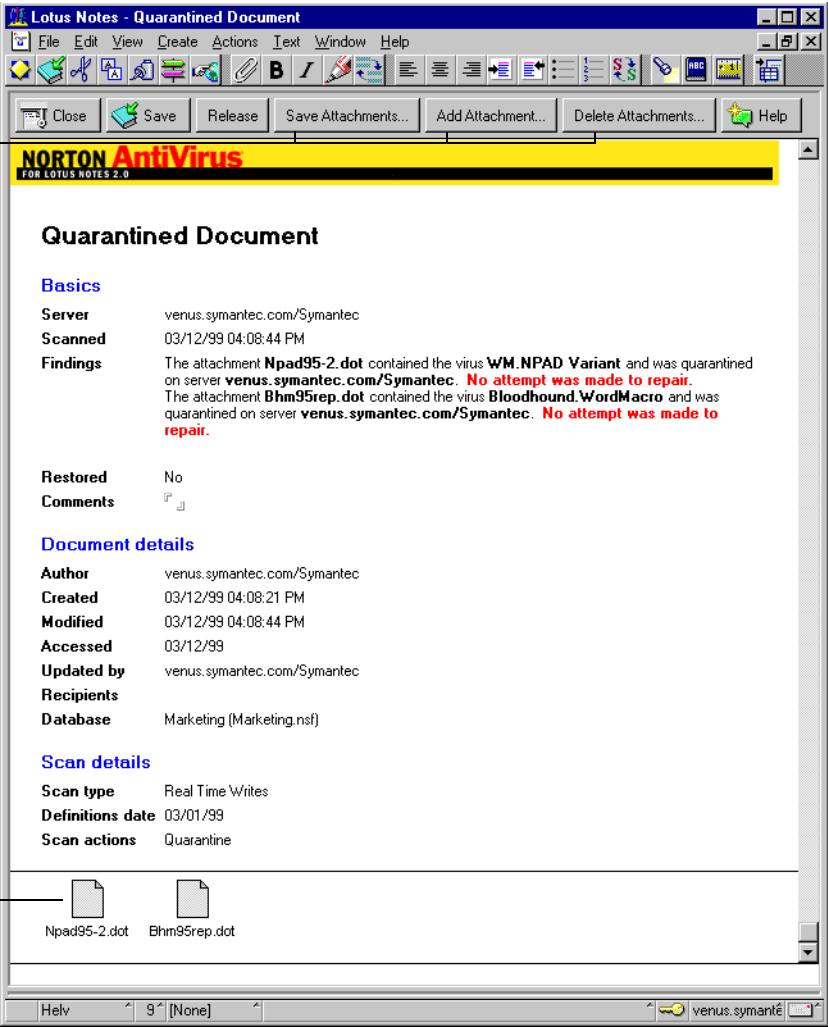
The infected document or email is deleted and the entry is removed from the Quarantine.

To manage infected attachments

- 1 Open the NAV Log and click Quarantine Documents.
- 2 Double-click an item in the Quarantine to view the Quarantine Item document.
- 3 Click one of the following:
 - **Save Attachments**
Saves the infected attachment as a file.
 - **Add Attachments**
Before releasing the document from the Quarantine, you can add a newly repaired compressed file, replace an infected file with a known good copy, or, perhaps, add a procedural file with instructions to scan a workstation.
 - **Delete Attachments**
Removes the infected attachments. You are prompted before the deletion takes place.

4 Click Release from Quarantine to release the document or email.

Actions for infected attachments



Attachments

Maintaining current protection

Norton AntiVirus relies on up-to-date information to detect and eliminate viruses. One of the most common reasons you may have a virus problem is that you have not updated your protection files since you installed the product. Symantec regularly supplies updated virus definitions files, which contain the necessary information about all newly discovered viruses.

About LiveUpdate

With LiveUpdate, Norton AntiVirus connects automatically to special Symantec sites and determines if your virus definitions need updating. If so, it downloads the proper files and installs them in the proper location.

LiveUpdate connects over the Internet to a site that Symantec maintains for LiveUpdate use. Generally, you do not have to do anything to configure LiveUpdate. The only requirement is an Internet connection.

If you do not want to permit direct access to the Internet from your Lotus Domino servers or are running proxy servers, you can set up an internal LiveUpdate server with LiveUpdate Administrator and configure Norton AntiVirus for Lotus Notes to access the internal LiveUpdate server instead. For more information, see [“Configuring for an internal LiveUpdate server”](#) on page 37.

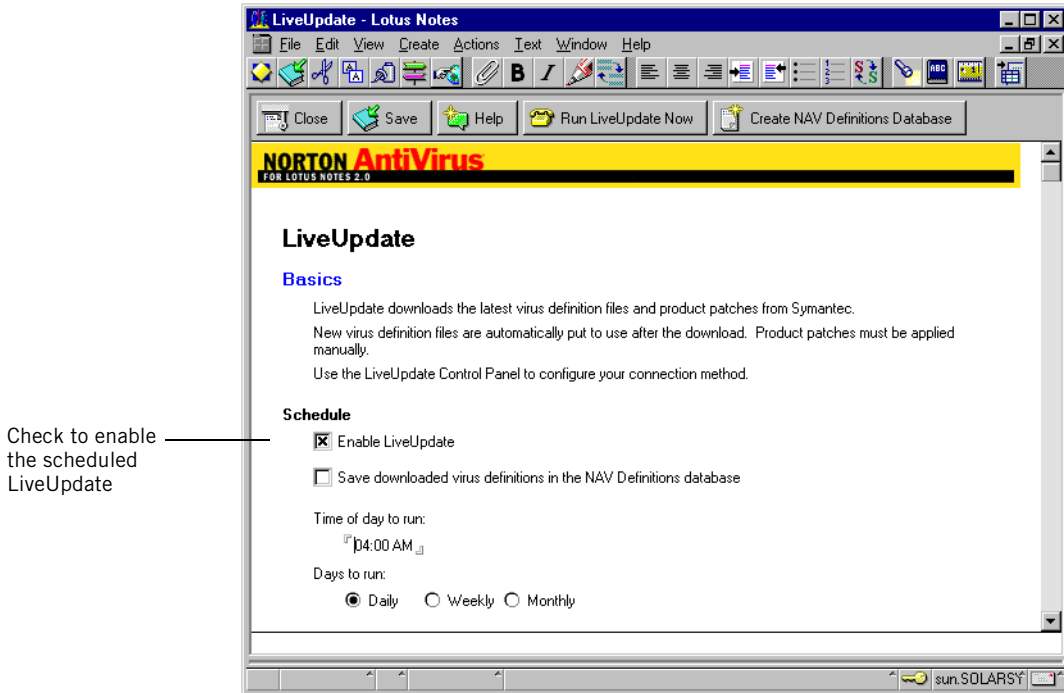
How to update virus protection

To immediately update virus definitions

- 1 In the Norton AntiVirus main window, click LiveUpdate.
The LiveUpdate form is displayed.
- 2 In the form, click the Run LiveUpdate Now button.

To schedule automatic LiveUpdates

- 1 In the Norton AntiVirus main window, click LiveUpdate.



- 2 In the Schedule section of the form, check Enable LiveUpdate.
Uncheck to disable LiveUpdate.
- 3 If you plan to replicate the virus definitions database to other Domino servers, check Save Downloaded Virus Definitions In The NAV Definitions Database.
Don't check this option if you have Norton AntiVirus installed on a single Domino server or do not plan to replicate the definitions database. See [“Replicating the NAV Definitions database”](#) on page 17 for more information.
- 4 Enter the time of day that LiveUpdate runs and select the frequency.
Specify an off-peak time for high-traffic networks.
- 5 At the top of the form, click Save, then Close.

Configuring for an internal LiveUpdate server

LiveUpdate operation is controlled by settings in the `/etc/liveupdate.conf` file. By default, an HTTP connection is made to the Symantec server. You can change the settings to point to an internal LiveUpdate server using either an FTP or HTTP protocol connection. The LiveUpdate server is created using the separately supplied and installed LiveUpdate Administration Utility.

To configure Norton AntiVirus for Lotus Notes to use an internal LiveUpdate server via FTP

- 1 For safety, make a backup copy of the following file:
`/etc/liveupdate.conf`
- 2 Make the following changes to the `liveupdate.conf` file:
 - Change the `protocol=` line to `protocol= ftp` for an FTP connection.
 - Change the `host=` line from `liveupdate.symantec.com` to your internal LiveUpdate server.
 - Change the `login=` and `password=` settings to the login and password for your FTP server.

Do not make changes to any other lines in the file.

To configure Norton AntiVirus for Lotus Notes to use an internal LiveUpdate server via HTTP

- 1 For safety, make a backup copy of the following file:
`/etc/liveupdate.conf`
- 2 Make the following changes to the `liveupdate.conf` file:
 - Change the protocol setting to `protocol=http`.
 - Change the `host=` line from `liveupdate.symantec.com` to your internal LiveUpdate server.

Do not make changes to any other lines in the file.

You can also configure `liveupdate.conf` to use a host (`.hst`) file created by the LiveUpdate Administration Utility (LUADMIN), which is a separately supplied program that runs on Windows NT. For more information, see the LiveUpdate Administration Utility document (`luadmin.pdf`) supplied with the LiveUpdate Administration Utility to configure the `.hst` file for use with Norton AntiVirus.

If you want to continue using an existing `liveupdt.hst` file from an earlier installation, make the following modification instead.

To use an existing liveupdt.hst file

- ◆ Add the following line to the /etc/liveupdate.conf file:
hostfile=<full path to the .hst file on the server>
If the hostfile= parameter is included in liveupdate.conf, all other lines are ignored and data from the .hst file is used instead.

To create a new liveupdt.hst file

- ◆ Use the separately supplied LiveUpdate Administration Utility (LUAdmin), which runs under Windows.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical Support

As part of Symantec Security Response, our global technical support group maintains support centers throughout the world. Our primary role is to respond to specific questions on product feature/function, installation and configuration, as well as author content for our Web accessible Knowledge Base. We work collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion such as working with Product Engineering as well as our Security Research Centers to provide alerting services and virus definition updates for virus outbreaks and security alerts.

Highlights of our offerings include:

- A range of support options gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components provide rapid response and up-to-the-minute information
- Software assurance delivers automatic software upgrade protection
- Content updates for virus definitions and security signatures ensure the highest level of protection

- Global support from Symantec Security Response experts is available 24x7 worldwide in a variety of languages
- Advanced features such as the Symantec Alerting Service and Technical Account Manager role offer enhanced response and proactive security support

Please reference our Web site for current information on Support Programs.

Registration and Licensing

If the product you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access our licensing and registration site at www.symantec.com/certificate. Alternatively you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product you wish to register, and from the Product Home Page select the Licensing and Registration link.

Contacting Support

Customers with a current support agreement may contact the Technical Support team via phone or Web at www.symantec.com/techsupp.

When contacting support please be sure to have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec
- Recent software configuration changes and/or network changes

Customer Service

Contact Enterprise Customer Service online at www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Updates to product registration such as address or name changes
- General product information (for example, features, language availability, dealers in your area)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to <http://service.symantec.com> and select your region under the Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

<http://www.symantec.com/>
(800) 721-3934

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

<http://www.service.symantec.com/mx>
+54 (11) 5382-3802

Asia/Pacific Ring

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucris Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

<http://www.service.symantec.com/br>
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico
Bldv Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

<http://www.service.symantec.com/mx>
+52 (5) 661-6120

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

<http://www.service.symantec.com/mx>

Subscription policy

If your Symantec product includes virus, firewall, or web content protection, you might be entitled to receive protection updates via LiveUpdate. The length of the subscription could vary by Symantec product.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

October 31, 2001

Index

A

- accessing
 - NAV Log 29
 - Norton AntiVirus 19
- Add Attachments option 33
- attachments 30
 - managing infections 33
 - viruses and 9
- automatic updates 36
- Auto-Protect
 - configuring 21-23
 - form 22
 - option 21

B

- Backup Documents log view 30
- Basics section 21
- Bloodhound technology 9, 27

C

- commands 20
- computer virus. *See* virus
- configuring
 - Norton AntiVirus 8
 - scans 21-28
- console commands 20
- current protection, maintaining 35-38

D

- definitions file, virus 9
- Delete Attachments option 33
- document backups 26, 30

E

- email, infected 32
- Excel. *See* Microsoft Excel

F

- forms
 - Auto-Protect scan 22
 - Global Options 25
 - Scan Now 24

G

- Global Options
 - form 25
 - processing 27
 - scan 26
 - virus detection notifications 28

H

- HELP command 20
- Help, online 19
- heuristic technology 9

I

- infected
 - attachments, managing 33
 - email 32
- initiating scans 21
- installation requirements 10
- installing Norton AntiVirus 10-18

J

- JOBS command 20

L

- LiveUpdate
 - automatic 36
 - description 9, 35
 - immediate update 35
 - replicating virus definitions database 17
 - scheduling 36
 - updating virus protection with 36

- log views 30
- logging options 24, 27
- Lotus Notes
 - partitions 11
 - server console window 20
 - virus threat 9

M

- macro virus 9
- maintaining protection 35-38
- managing
 - infected attachments 33
 - Quarantine 31-34
 - Quarantine items 32
- Microsoft Excel 9
- Microsoft Word 9
- MIME options 27

N

- NAV Log
 - accessing 29
 - replicating 15
 - using 28-34
- NAV Settings, replicating 15
- Norton AntiVirus
 - accessing 19
 - Bloodhound technology 9, 27
 - commands 20
 - configuration 8
 - configuring scanning 21-28
 - console commands 20
 - description 8-9
 - functions 9
 - getting started 19
 - help 19
 - installing 10-18
 - LiveUpdate 9
 - maintaining protection 35-38
 - system requirements 10
- Notes. *See* Lotus Notes
- Notifications section 21

O

- online Help 19
- operating system requirements 10
- options
 - logging 27
 - MIME 27
 - processing 27
 - scanning 21
 - virus detection notifications 28

P

- processing options 27
- protection
 - maintaining 35-38
 - updating
 - with LiveUpdate 35

Q

- Quarantine
 - infected attachments 33-34
 - items 32
 - managing 31-34
- Quarantined Documents log view 30
- QUIT command 20

R

- Readme.txt file 12
- replicating
 - NAV log 15
 - NAV settings 15
 - virus definitions database 17
- requirements, system 10

S

- Save Attachments option 33
- SCAN command 20
- Scan Now
 - configuring 21
 - form 24
 - option 21
- Scan Reports log view 30

scanning

- Auto-Protect form 22
- configuring 21-34
- initiating 21
- notifications 21
- options 21, 24-28
- Scan Now form 24
- Scheduled Scan
 - configuring 21, 23
 - multiple servers 24
 - option 21
- scheduling LiveUpdate 36
- scheduling scans 23
- Server Messages log view 30
- Service and Support 39
- signature, virus 9
- starting Norton AntiVirus 19
- STOP command 20
- Symantec
 - Web site 9
- system requirements 10

T

- Technical Support 39

U

- updating
 - virus protection
 - with LiveUpdate 35
- using NAV Log 28-34

V

- virus
 - as attachment 9
 - definition 8
 - definitions file 9
 - Lotus Notes 9
 - macro virus 9
 - program virus 9
 - signature 9
 - updating protection
 - with LiveUpdate 35
- virus definitions database, replicating 17
- virus detection notifications 28
- Virus Incidents log view 30

W

- Web site, Symantec 9
- Word. *See* Microsoft Word